CERTIFICATE OF MAILING BY "EXPRESS MAIL"

"Express Mail" Mailing Label Number: EL843735584US

Date of Deposit: November 18, 2003

I hereby certify that this correspondence is being deposited with the United States Postal "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Mail Stop Patent Application, Commissioner for Patents, PO Box 1450, Alexandria, Virginia 22313-1450.

U.S. Patent Application for Juergen Plessmann entitled "METHOD AND DEVICE FOR THE REMOTE TRANSMISSION OF SENSITIVE DATA, a letter under 37 CFR 1.41(c), two sheets of drawings containing two Figures, an unsigned Declaration, a Certified Copy of German 102 53 676.7 and appropriate government filing fee. (Attorney's Docket No. P03,0424).

John Lanson

Signature of Person Mailing Application and Fees

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	102 53 676.7
Anmeldetag:	18. November 2002
Anmelder/Inhaber:	Siemens Aktiengesellschaft, München/DE
Bezeichnung:	Verfahren und Vorrichtung für die Fernübertragung sensibler Daten
IPC:	H 04 L 12/22

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 02. Oktober 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Ebert

A 9161
06/00
EDV-L

Beschreibung

Verfahren und Vorrichtung für die Fernübertragung sensibler Daten

Die Erfindung betrifft ein Verfahren und eine Vorrichtung für die Fernübertragung sensibler Daten. Unter sensiblen Daten sollen dabei solche Daten verstanden werden, die teilweise geheimhaltungsbedürftig sind, also geheimhaltungsbedürftige Datenbestandteile enthalten.

Die moderne Kommunikationstechnologie ermöglicht die Übertragung vielfältigster Daten zwischen verschiedenen Orten. Zur Verarbeitung und Übertragung der Daten werden in aller Regel Rechner benutzt, die über lokale Netzwerke, Telefonverbindungen, kabellose Schnittstellen oder das Internet miteinander verbunden sein können. Die Übertragung von Daten über diese Verbindungen ist meist abhörbar und es existiert eine Vielzahl von Mechanismen zu deren kryptografischem Schutz. Diese Mechanismen zielen entweder darauf ab, den gesamten Kommunikationsweg zu schützen, oder sie dienen der Verschlüsselung von kompletten Dateien bzw. Datenbanken.

Ein wirksamer Schutz von Daten ist insbesondere auf dem Gebiet der Medizin, in Forschung und Entwicklung sowie im Finanzgewerbe gefragt. Auf diesen Gebieten ist die Kommunikation von Daten eminent wichtig, ebenso die Verwendung von Rechnern zur Verarbeitung von Daten. Die Rechnersysteme und Kommunikationswege sind weitestgehend kryptografisch gegen Aushorchung geschützt.

Aufgrund der Vielzahl im Einsatz befindlicher Rechnersysteme, die teilweise hoch komplex sind, sind intensive Wartungsmaßnahmen nicht zu vermeiden. Diese können auch unvorhergesehen und in unregelmäßigen Zeitabständen erforderlich werden, z.B. bei Auftreten von Fehlern. Abhängig davon, welche Teile des Rechnersystems von Fehlern betroffen sind, kann es erforder-

lich sein, bei der Wartung auch Anwendungen, die sensible Daten verarbeiten, beispielsweise einem Wartungstechniker zu zeigen. Dies kann bereits bei einer Wartungsmaßnahme vor Ort nicht akzeptabel sein, falls der Wartungstechniker nicht zu einem für die Kenntnis der sensiblen Daten autorisierten Kreis von Personen gehört. Um so kritischer ist der Umstand bei Fernwartungsmaßnahmen zu beurteilen, bei dem beispielsweise Funktionen von Anwendungsprogrammen oder Bildschirminhalte über grundsätzlich ungeschützte Kommunikationswege übertragen werden müssen.

Zum Beispiel kann es erforderlich sein, bei der medizinischen Untersuchung eines Patienten mit einem rechnergesteuerten Diagnosegerät einen Wartungsfachmann hinzuzuziehen, um eine Optimierung oder das Beheben von Fehlern im System zu ermöglichen, die während der rechnergestützten diagnostischen Anwendung auftreten. Ähnliche Problemstellungen können sich beispielsweise ergeben, wenn Fehler in einer rechnergestützten Finanzanwendung auftreten, die dem Wartungsfachmann im laufenden Betrieb vorgeführt werden müssen. Bei der Einsichtnahme in laufende Systeme ist es unvermeidlich, dass auch geheimhaltungsbedürftige Datenbestandteile einsehbar werden.

Neben der Wartung kann die Einsichtnahme in die Rechnersysteme auch zu Schulungszwecken erforderlich sein, um die Bedienung komplexer Anwendungen demonstrieren zu können. Dies ist häufig nur dann möglich, wenn ein Datenbestand zur Verfügung steht, mit dem die Anwendung arbeiten kann, ohne dass es auf den tatsächlichen Inhalt der Daten ankäme. Die Schulung von Personen, die nicht zur Einsichtnahme in den Datenbestand autorisiert sind, verbietet sich dann jedoch von selbst..

Weiter kann die Einsichtnahme gerade in medizinischen Umgebungen auch im Rahmen von sogenannten Expertensystemen erforderlich sein, bei denen andere klinische Experten zur Beurteilung klinischer Daten herangezogen werden. Dabei ist es erforderlich, dass dem herangezogenen Experten Daten wie dia-

gnostische Aufnahmen oder die Pathogenese eines Patienten zugänglich gemacht werden. Dadurch werden zwangsläufig personenbezogene Daten der Patientenakte mit übertragen und dadurch möglicherweise auch nicht autorisierten Betrachtern der Daten mitgeteilt.

Ein besonders schneller und effizienter Datenaustausch findet meist über eine Datenfernübertragung statt. Dies gilt für Schulungsmaßnahmen und Expertensysteme ebenso wie für Fernwartungsmaßnahmen, durch die Wartezeiten bis zum Erscheinen des Wartungspersonals vor Ort vermeidbar sind. Außerdem können auch für Wartungsfachleute Expertensysteme nutzbar gemacht werden. Zur Fernwartung stehen Möglichkeiten zur Verfügung, die Daten in einem Anwendungsrechner durch einen entfernt arbeitenden Wartungsfachmann einzusehen. Dies schließt die Einsichtnahme in Festplattendaten ebenso wie in laufende Prozessdaten im Arbeitsspeicher ein, zudem können auch Bildschirminhalte übertragen werden, um aktuelle Meldungen einsehbar zu machen und das Bildschirmgeschehen gemeinsam nachvollziehen zu können. Die Fernwartung spezieller Anwendungen setzt dabei voraus, dass sowohl beim Anwendungsrechner als auch beim entfernten Wartungsrechner kompatible Hardware und Software vorhanden ist.

Mit den Möglichkeiten der Fernwartung insbesondere medizinisch-diagnostischer Geräte, die rechnergestützt arbeiten, z.B. CT-Tomographen, MR-Scanner oder Bildarchiv-Workstations, setzt sich die DE 196 51 270 C2 auseinander. Dort werden Lösungen vorgeschlagen, um die Fernwartung flexibel zu gestalten, indem einheitlich gemeinsame Programmiersprachen wie z.B. HTML verwendet werden. Eine Möglichkeit, die Betrachtung sensibler Daten durch den Wartungstechniker zu verhindern, wird jedoch nicht angeboten.

Die Aufgabe der Erfindung besteht darin, eine Möglichkeit zur Einsichtnahme in rechnergestützt arbeitende Anwendungen zu geben, die dem Einsichtnehmenden einen möglichst umfassenden

Einblick in die Daten und Prozesse des Anwendungsrechners gestattet, ohne jedoch gleichzeitig die Möglichkeit zur Einsicht in geheimhaltungsbedürftige Daten zu schaffen.

Die Erfindung löst diese Aufgabe durch ein Verfahren mit den Merkmalen des ersten Patentanspruchs und durch eine Vorrichtung mit den Merkmalen des achten Patentanspruchs.

Ein Grundgedanke der Erfindung besteht darin, sämtliche Daten in einer rechnergestützten Anwendung zwar zur Betrachtung oder Fernübertragung zur Verfügung zu stellen, gleichzeitig jedoch sämtliche geheimhaltungsbedürftigen Datenbestandteile von der Übertragung oder Betrachtung auszuschließen. Dadurch kann ein Betrachter an einem Rechner, an den die Daten übertragen werden, sämtliche Daten und Prozesse der rechnergestützten Anwendung einsehen und verfolgen. Gleichzeitig ist ihm jedoch die Möglichkeit zur nicht berechtigten Einsichtnahme in geheimhaltungsbedürftige Datenbestandteile verwehrt. Unter sämtlichen Daten sollen dabei jegliche im Rechner verfügbaren Informationen verstanden werden, z.B. Festspeicherinhalte, Arbeitsspeicherinhalte oder Bildschirm-Anzeigeinhalte. Unter geheimhaltungsbedürftigen Datenbestandteilen sollen Daten wie Name, Alter, Adresse von Personen, ID's, UID's, Schlüsselkennzeichen, Sozialversicherungsnummer, Bankkontodaten, Finanzinformationen oder Umfragedaten verstanden werden.

In einer vorteilhaften Ausgestaltung der Erfindung werden die geheimhaltungsbedürftigen Datenbestandteile je nach Bedarf entweder gelöscht, anonymisiert oder pseudonymisiert. Dabei soll unter Anonymisieren jegliche Unkenntlichmachung personenbezogener Datenbestandteile verstanden werden, durch die Einzelangaben über persönliche oder sachliche Verhältnisse nicht oder nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft der zugehörigen Person zugeordnet werden können. Unter Pseudonymisierung soll die Unkenntlichmachung des Namens und anderer Identifikationsmerkmale durch

ein Kennzeichen, um die Identifikation der betroffenen Person auszuschließen oder wesentlich zu erschweren. Dies hat den Vorteil, dass je nach Anwendung entsprechende Datenfelder entweder leer oder aber durch anonyme bzw. pseudonyme Anzeigeelemente befüllt sind, die dem Betrachter einen Hinweis darauf geben, welche Art von Information an der jeweiligen Stelle platziert ist und an welchen Stellen Information zwar vorhanden, aber nicht einsehbar ist.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung werden geheimhaltungsbedürftige Datenbestandteile auch aus Bildschirminhalten oder den Inhalten anderer Anzeigeelemente eliminiert. Dadurch ergibt sich der Vorteil, dass ein entfernt sitzender Betrachter zur Analyse eines vor Ort arbeitenden Systems auch interaktive Vorgänge auf dem Bildschirm einsehen und mitverfolgen kann, ohne dabei Zugang zu geheimhaltungsbedürftigen Daten zu erhalten.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung erfolgt die Fernübertragung von Daten auf Anforderung eines entfernt angeordneten Rechners, bei dem es sich um einen Arbeitsplatz eines Service-Dienstleisters handelt, der eine Fernwartung des vor Ort arbeitenden Rechners vornehmen will. Dadurch kann trotz Vorhandensein geheimhaltungsbedürftiger Daten sichergestellt werden, dass das Wartungspersonal jeglichen hochspezialisierten Wartungsservices ohne Rücksichtnahme auf den jeweiligen Autorisierungs-Status in Anspruch genommen werden kann. Insbesondere ergibt sich die Möglichkeit zur schnellen und effizienten Fernwartung von Anwendungsrechnern mit geheimhaltungsbedürftigen Daten auch durch wechselnde Wartungsservices. Die Nutzung wechselnder, unterschiedlicher Wartungsservices kommt in der praktischen Anwendung häufig vor.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung wird die Eliminierung geheimhaltungsbedürftiger Datenbestandteile durch ein Datenschutzmodul vorgenommen, das als Karte

in einem Anwendungsrechner integrierbar oder als eigenständiges Gerät an einen Anwendungsrechner anschließbar ist. Dadurch ergibt sich der Vorteil, dass nahezu jeder Rechnerarbeitsplatz bei Bedarf modular mit dem Datenschutzmodul ausgestattet werden kann. So kann auch eine nachträgliche Ausstattung bzw. die Anpassung der Funktionalität des Anwendungsrechners bei wechselnden Anwendungsgebieten erfolgen.

Weitere vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der abhängigen Patentansprüche.

Nachfolgend werden Ausführungsbeispiele der Erfindung anhand von Figuren erläutert. Es zeigen:

Figur 1 Rechnersystem mit Datenschutz-Modulen gemäß der Erfindung,

Figur 2 Verfahren zur Ausführung der Erfindung.

Figur 1 zeigt ein Rechnersystem mit Daten-Schutzmodulen 13 gemäß der Erfindung. Das Rechnersystem ist eingebunden in eine Arbeitsumgebung 1, in der mit sensiblen Daten gearbeitet wird, z.B. eine klinische Umgebung, eine Umgebung im Finanzwesen oder in einem Umfrageinstitut. In dieser Arbeitsumgebung 1 ist eine Workstation 3 als Befundungs-Arbeitsplatz installiert, die über einen Bildschirm 4 verfügt und an der die Bearbeitung, Speicherung, Archivierung oder Verfügbarmachung sensibler Daten erfolgt.

Soweit die sensiblen Daten anderen Arbeitsplätzen innerhalb der Arbeitsumgebung 1 zur Verfügung gestellt werden, geschieht dies über Kommunikationswege, die in Figur 1 nicht näher dargestellt sind, und die speziellen Datenschutzauflagen der Arbeitsumgebung genügen. Die Workstation 3 verfügt jedoch auch über einen Anschluss an Kommunikationswege, die den Austausch von Daten über Kommunikationswege außerhalb der Arbeitsumgebung 1 erlauben. Die Anbindung an diese Kommunika-

tionswege erfolgt über ein Modem 9, wobei unter Modem hier ein Telefonmodem ebenso wie ein Funkmodem oder eine Netzwerkverbindung verstanden werden kann.

Da die Workstation 3 Zugriff auf sensible Daten hat, muss der unberechtigte Zugriff auf die Workstation 3 über das Modem 9 durch das Datenschutzmodul 13 kontrolliert bzw. unterbunden werden. Datenzugriffe erfolgen dabei nur auf eine Anforderung zur Fernübertragung oder Betrachtung hin, die das Datenschutzmodul 13 in Aktion treten lassen. Auf diese Anforderungen hin wird kein direkter Zugriff auf die sensiblen Daten gewährt, sondern das Datenschutzmodul 13 als Zwischeninstanz aktiviert. Die Aktivierung des Datenschutzmoduls 13 kann dabei rollenabhängig erfolgen, d.h. abhängig von der Identität des Anfordernden, oder abhängig vom jeweiligen Datenzugang, d.h. abhängig von der internen oder externen Position des Anfordernden, oder abhängig von der Eingabe eines Benutzers, der das Datenschutzmodul 13 direkt aktivieren kann.

Das Datenschutzmodul 13 und das Modem 9 können in die Workstation als Steckkarten oder Einschübe integriert sein und einen gemeinsamen hardwaremäßigen Aufbau bilden, was durch die gestrichelte Umrahmung 2 angedeutet ist. Die Komponenten können jedoch ohne Beeinträchtigung der Funktion als eigenständige Geräte an die Workstation extern angeschlossen sein, außerdem können Datenschutzmodul 13 und Modem 9 ihrerseits als gemeinsame Komponente integriert sein, was in der Figur nicht dargestellt ist. Außerdem kann das Datenschutzmodul 13 auch ein in die Workstation 3, in einen davon getrennten Server oder in das Modem 9 integriertes Software-Modul sein. Darüber hinaus kann auch die Abfolge von Datenschutzmodul 13 und Modem 9 vertauscht sein, so dass das Modem 9 unmittelbar an die Workstation 3 angeschlossen ist und über das Datenschutzmodul 13 Verbindung zu den Kommunikationswegen außerhalb der Arbeitsumgebung hat.

In der Arbeitsumgebung 1 können weitere rechnergestützte Arbeitsplätze installiert sein, die ebenfalls mit sensiblen Daten arbeiten, z.B. eine Modalität 5, die der Erzeugung medizinisch-diagnostischer Bilddaten dient, oder ein klinischer Arbeitsplatz 7, der die Bearbeitung von Befunddaten und Medikationen mittels elektronischer Patientenakten ermöglicht. Weitere und je nach Arbeitsumgebung getrennt verschiedene rechnergestützte Anwendungen sind denkbar, die allesamt mit sensiblen Daten arbeiten und innerhalb der Arbeitsumgebung 1 über in der Figur 1 nicht dargestellte Datennetze miteinander verbunden sein können. Für jeden dieser Arbeitsplätze kann eine durch ein Datenschutzmodul 13 geschützte Datenverbindung zu außerhalb der Arbeitsumgebung 1 verlaufenden Kommunikationswegen 11 über ein Modem 9 hergestellt werden.

Soweit die Datenverbindungen zu externen Kommunikationswegen 11 dem Austausch sensibler Daten einschließlich der geheimhaltungsbedürftigen Datenbestandteile dienen, finden kryptografische Datenschutzmechanismen Verwendung, die nicht Gegenstand der Erfindung sind. Es gibt jedoch eine Vielzahl von Datenverbindungen, die zwar zum Austausch der sensiblen Daten, nicht jedoch der geheimhaltungsbedürftigen Datenbestandteile, hergestellt werden. Eine Anwendung solcher Datenverbindungen kann die Einsichtnahme in Daten im Rahmen eines Expertensystems sein, bei dem klinische Experten außerhalb der Arbeitsumgebung 1 hinsichtlich der nicht geheimhaltungsbedürftigen Datenbestandteile konsultiert werden sollen, dazu jedoch die geheimhaltungsbedürftigen Datenbestandteile nicht benötigen. Datenverbindungen sind auch zu anderen Zwecken denkbar, z.B. zum Austausch allgemeiner Informationen aus den Anwendungen heraus oder zur Herstellung von persönlich nutzbaren Kommunikationsverbindungen für das Versenden von Email oder Übertragen von Dateien, die keinen direkten Bezug zu den Anwendungen haben, jedoch Zugriffsmöglichkeiten auf den Rechner innerhalb der Arbeitsumgebung 1 eröffnen.

Datenverbindungen nach außerhalb der Arbeitsumgebung 1 können insbesondere auch der Fernwartung der rechnergestützten Anwendungen dienen, bei der z.B. die Versionsnummer installierter Software von außen abgefragt wird, Software von außen zugespielt wird, Fehlermeldungen von außen eingesehen oder ein optimierungsbedürftiges Rechnerverhalten von außen beobachtet werden kann. Derartige Fernwartungsmaßnahmen sind allgemein üblich, da die Einsichtnahme über elektronische Datenverbindungen schnell erfolgen kann und gegebenenfalls auch die Konsultation weiterer Wartungsfachleute in einem Fernwartungs-Servicezentrum ermöglicht. Die Wartung bezieht sich dabei jeweils auf die installierte Hardware oder Software und deren Funktionsweise, weswegen gegebenenfalls Anwendungsprogramme gestartet werden müssen. Dabei sollte jedoch keine Einsichtnahme durch Wartungsfachleute in geheimhaltungsbedürftige Daten erfolgen, um von deren Autorisierungs-Status unabhängig arbeiten zu können.

Soweit eine Fernwartung der Anwendungsrechner der Arbeitsumgebung 1 erfolgen soll, kann diese aus einem Fernwartungs-Zentrum 15 heraus erfolgen, das beispielsweise vom Hersteller der Software oder von einem speziellen Wartungsunternehmen betrieben wird. Die Verbindung zu einem solchen Wartungszentrum 15 erfolgt über die öffentlichen Kommunikationswege 11, mit denen das Fernwartungszentrum 15 ebenso über ein Modem 9 verbunden ist. Die Verbindung wird hergestellt von einer Wartungs-Workstation 17 mit Bildschirm 19, von der ein Wartungsfachmann Zugriff auf den zu wartenden Rechner, die darauf installierte Software und alle nicht durch das Datenschutzmodul 13 geschützten Daten darauf hat. Im Rahmen dieses Zugriffs können Daten eingesehen werden, Anwendungen auf dem Anwendungsrechner 3, 5, 7 gestartet werden, die Bildschirminhalte des Anwendungsbildschirms 4 betrachtet werden oder Wartungsprogramme am Anwendungsrechner 3, 5, 7 oder auf der Wartungsworkstation 17 gestartet werden.

Der Wartungszugriff ist jedoch nicht nur aus einem Servicezentrum 15 heraus möglich, sondern auch von anderen Servicerechnern aus, z.B. von einem Notebook 21, das ebenfalls über ein Modem 9 mit dem Anwendungsrechner 3, 5, 7 Verbindung aufnehmen kann. Dabei stehen dieselben Funktionalitäten wie aus dem Servicezentrum 15 heraus zur Verfügung, was insbesondere die Betrachtung der Bildschirminhalte des Anwendungsbildschirms 4 am Notebookbildschirm 23 beinhaltet. Die Wartung durch ein Notebook 21 oder ein ähnliches portables Gerät erlaubt jedoch auch einen Wartungseinsatz vor Ort, der insbesondere bei der Berücksichtigung von Hardware-Fragen zu Wartungszwecken erforderlich sein kann. Zu diesem Zweck gestattet das Modem 9 das Herstellen einer Datenverbindung nicht nur über öffentliche Kommunikationswege 11, sondern auch in direkter Verbindung zu einem entsprechenden Modem oder Anschluss am Anwendungsrechner 3, 5, 7. Auch ein derartiger Wartungszugriff vor Ort in der Arbeitsumgebung 1 wird jedoch durch ein Datenschutzmodul 13 geschützt, da der Wartungsfachmann auch vor Ort keinen Einblick in geheimhaltungsbedürftige Daten erhalten darf.

Die Verwendung eines Wartungs-Notebooks 21 über eine durch ein Datenschutzmodul 13 geschützte Verbindung ermöglicht es dabei, einen Anbindungsrechner zu warten, ohne dessen Anwendungsbildschirm 4 einsehen zu müssen, auf dem geheimhaltungsbedürftige Daten angezeigt sein können. Statt dessen besteht jedoch auch die Möglichkeit, die auf dem Anwendungsbildschirm 4 dargestellten Inhalte ebenfalls durch das Datenschutzmodul 13 schützen zu lassen, falls eine Wartung erfolgen soll. Zu diesem Zweck muss das Datenschutzmodul 13 in den Anwendungsrechner 3 bzw. in die Verbindung zwischen Anwendungsrechner 3 und Anwendungsbildschirm 4 integriert sein. Der Datenschutz für Bildschirminhalte kann dann mittels Knopfdruck aktiviert werden, falls eine Wartung erfolgen soll.

Das Datenschutzmodul 13 übernimmt die Aufgabe, die Einsichtnahme in geheimhaltungsbedürftige Datenbestandteile zu ver-

hindern. Dabei sollen jedoch Anwendungsprogramme, die auf geheimhaltungsbedürftigen Daten basieren, ausführbar bleiben und sonstige Dateninhalte des Rechners zu Analyse frei zugänglich sein. Dies ist insbesondere zur Optimierung oder Wartung von Anwendungsprogrammen erforderlich, soweit Schwächen oder Fehler zu analysieren sind, die nur im Betrieb der Anwendungsprogramme unter Verwendung sensibler Daten beobachtbar sind. Zu diesem Zweck können über das Datenschutzmodul 13 grundsätzlich sämtliche Daten und Bildschirminhalte übertragen werden. Vor der Übertragung identifiziert das Datenschutzmodul 13 jedoch geheimhaltungsbedürftige Datenbestandteile der zu übertragenden Daten. Solche Datenbestandteile können insbesondere sämtliche persönlichen oder demographischen Informationen sein, z.B. der Name von Patienten oder Kunden, ID's, UID's, Schlüsselkennzeichen, Sozialversicherungsnummer, das Geburtsdatum, die Adresse, Bankverbindungen, Informationen zum finanziellen Status oder Ergebnisse von kritischen Umfragen oder statistischen Auswertungen. Von besonderer Bedeutung ist die Geheimhaltung persönlicher Informationen im medizinischen Umfeld, wo in Form elektronischer Patientenakten vollständige Informationen zur Persönlichkeit, Pathogenese und Diagnose von Patienten vorliegen. Hier wird mit sehr komplexen Anwendungsrechnern an besonders sensiblen Daten gearbeitet. Gleichzeitig ist der optimale Zustand der Anwendungsrechner im medizinischen Umfeld eine zwingende Voraussetzung, die eine besonders effiziente und intensive Wartung der Systeme unumgänglich macht.

Bei der Übertragung von Patientenakten oder Dateien vorgegebener Formate identifiziert das Datenschutzmodul 13 Datenfelder innerhalb der Dateien oder Akten, die geheimhaltungsbedürftige Datenbestandteile enthalten. Dazu hat das Datenschutzmodul 13 Zugriff auf einen integrierten oder angeschlossenen Speicher, der eine Zuordnung von Datenformaten und darin enthaltenen, geheimhaltungsbedürftigen Datenfeldern enthält, bzw. die Erkennung solcher Datenfelder an den Datenfeld-Kennzeichnungen ermöglicht. Der Speicher kann insbeson-

dere ein in das Datenschutzmodul 13 integrierter, nicht löschbarer Speicher, z.B. ein Flash, ein EPROM oder ein EEPROM sein. Es kann sich jedoch auch um eine Festplatte handeln. Soweit Dateien oder elektronische Akten übertragen werden, erfolgt dies über ein Kommunikationsprotokoll, das durch das Datenschutzmodul 13 unterstützt wird, z.B. TCPIP oder FTP. Darüber hinaus unterstützt das Datenschutzmodul 13 die Dateiformate der zu übertragenden Daten. Eine Übertragung von Daten in nicht unterstützten Dateiformaten oder Kommunikationsprotokollen ist nicht möglich.

Das Datenschutzmodul 13 hat weiter Zugriff auf eine Referenzdatenbank, die geheimhaltungsbedürftige Daten enthält. Damit ist es möglich, die zu übertragenden Daten mit dem Inhalt der Referenzdatenbank zu vergleichen, um geheimhaltungsbedürftige Datenbestandteile zu erkennen. Die Referenzdatenbank kann dabei Daten enthalten, die beim Anlegen von Dateien und Akten innerhalb der Arbeitsumgebung 1 einen Vermerk erhalten, der auf die Geheimhaltungsbedürftigkeit hinweist. Dieser Vermerk bewirkt, dass die entsprechenden Daten in die Referenzdatenbank gefüllt werden. In einem Datenbanksystem könnten die entsprechenden Daten in der Referenzdatenbank gespeichert werden und von den Anwendungen jeweils aus dieser Datenbank abgerufen werden. Bei der Referenzdatenbank kann es sich z.B. um eine Personendatenbank handeln, zu deren Schutz gesonderte Datenschutzmaßnahmen angesetzt werden können. Das Datenschutzmodul 13 unterbindet die Übertragung von Daten, die in der Referenzdatenbank vorkommen, vollständig.

Die Referenzdatenbank kann auch eine Liste möglicher geheimhaltungsbedürftiger Informationen enthalten, die unabhängig von der Arbeitsumgebung 1 angelegt ist. Beispielsweise kann zum Schutz personenbezogener Daten eine Referenzdatenbank installiert sein, die ein Verzeichnis sämtlicher bekannter Vornamen und Nachnamen enthält, und zwar unabhängig davon, ob der jeweilige Name in der Arbeitsumgebung 1 verwendet wird oder nicht. Damit ist gewährleistet, dass das Datenschutzmo-

dul 13 durch Vergleich mit der Referenzdatenbank die Übertragung jeglichen Namens unterbinden kann. In vergleichbarer Weise kann eine Referenzdatenbank sämtlicher medizinisch-diagnostischer Befunde, kritischer Begriffe des Finanzwesens oder kritischer demographischer Begriffe angelegt sein.

Das Datenschutzmodul 13 hat weiter Zugriff auf einen Speicher, in dem Suchmasken für geheimhaltungsbedürftige Datenbestandteile angelegt sind. Dabei kann es sich z.B. um Datumssuchmasken für gängige Datumsformate handeln, wie ##.##.####, ##/##/## oder ##.mmm.####. Es können auch Suchmasken für Adressangaben angelegt sein, die z.B. typische Kombinationen von Straßenname und Straßennummer oder Postleitzahl und Ort sowie Landesangaben erkennen. Außerdem können Suchmasken für Umsatzdaten anhand der Angabe von Währungen erkannt werden oder Suchmasken zum Ausschluss jeglicher Ziffer oder jeglichen Buchstabens verwendet werden.

Weiter unterstützt das Datenschutzmodul 13 auch die Übertragung von Daten, die Bildschirminhalte oder Videoframes repräsentieren. Diese aktuell angezeigten oder im Graphikspeicher gespeicherten Bildschirmdarstellungen können ebenfalls zu Zwecken der Fernwartung oder Schulung oder ganz einfach Einsichtnahme übertragen werden, um z.B. interaktive Prozesse oder Bildschirmmeldungen fern einsehbar zu machen. Da sie geheimhaltungsbedürftige Datenbestandteile des Anwendungsrechners 3, 5, 7 beinhalten können, ist ihre Übertragung ebenfalls vor unberechtigter Einsichtnahme zu schützen.

Dazu verfügt das Datenschutzmodul über Routinen, die die Erkennung dieser Datenbestandteile auch in Bildschirminhalten ermöglichen. Die Bildschirminhalte liegen jedoch nicht in üblichen Datenformaten, wie z.B. ASCII vor, sondern müssen eigens durch Datenerkennungsprogramme analysiert werden. Zu diesem Zweck werden die Bildschirmdaten in analoger Weise wie bei OCR-Programmen so weit möglich in ASCII-Daten zurückverwandelt, soweit sie nicht in ASCII-verwandten Datenformaten

übertragen werden. Die ASCII-verwandten oder in ASCII zurück überführten Bildschirminhalte werden ebenso wie die zu übertragenden Dateien und elektronischen Akten unter Verwendung von Suchmasken oder Referenzdatenbanken auf geheimhaltungsbedürftige Datenbestandteile durchsucht. Das Datenschutzmodul 13 behandelt Bildschirminhalte und Videoframes also in vergleichbarer Weise wie Dateien und elektronische Akten. Geheimhaltungsbedürftige Datenbestandteile, die durch das Datenschutzmodul 13 erkannt werden, werden aus dem zu übertragenden Daten entweder gelöscht, anonymisiert oder pseudonomysiert.

Bildschirminhalte können zusätzlich in wesentlich einfacherer Weise vor deren Darstellung auf dem Bildschirm 19, 23 geprüft und geschützt werden. Dazu identifiziert das Datenschutzmodul 13 geheimhaltungsbedürftige Datenbestandteile bereits vor deren Sichtbarmachung der darzustellenden Daten und eliminiert sie. Das Aufbauen von Bildschirminhalten erfolgt dann erst im Anschluss an die Bearbeitung durch das Datenschutzmodul 13. Dadurch wird ein zuverlässiger Schutz der sensiblen Daten auch bei Übertragung von Bildschirminhalten gewährleistet, ohne dass besondere Routinen z.B. zum Analysieren von Pixelbasierten Video-Frames erforderlich wären.

Insbesondere bei Übertragung von Dateien oder Akten mit fest vorgegebenen Datenfeldern führt das Löschen von Datenbestandteilen dazu, dass der Empfänger Dateien mit teilweise leeren Datenfeldern enthält. Durch die fest vorgegebenen Formate der Dateien oder Akten wird der Kontext der Information durch Löschung jedoch nicht verändert, so dass die übertragenen Informationen für den Empfänger gut lesbar bleiben. In bestimmten Situationen kann es jedoch erforderlich sein, dass der Empfänger einen Hinweis darauf enthält, dass und an welcher Stelle Datenbestandteile von der Übertragung ausgeschlossen wurden. Zu diesem Zweck verfügt das Datenschutzmodul 13 über Routinen, die die von der Übertragung auszuschließenden Daten

nicht löschen sondern entweder anonymisieren oder pseudonymisieren.

Bei der Anonymisierung sollen jegliche personenbezogene Datenbestandteile über persönliche oder sachliche Verhältnisse unkenntlich oder nicht mehr zuordenbar gemacht werden. Dazu kann z.B. anstelle der gelöschten Daten eine Zensur-Maske überblendet werden, z.B. anstelle jeder gelöschten Ziffer eine Raute oder anstelle jedes gelöschten Buchstabens ein x. Außerdem sind Unkenntlichmachungen in Form von Schwärzungen oder vom Inhalt unabhängigen Zensurmasken möglich. Bei der Pseudonymisierung werden Namen und andere Identifikationsmerkmale durch ein Kennzeichen ersetzt, um die Identifikation der betroffenen Person unmöglich zu machen. Anstelle der personenbezogenen Datenbestandteile wird also jeweils ein Pseudonym übertragen, z.B. „Max Mustermann", „Prename Name" oder „ID" oder „UID".

Sowohl Anonymisierung als auch besonders Pseudonymisierung signalisieren dem Empfänger der übertragenen Daten zum einen, welche Art von Daten von der Übertragung ausgeschlossen wurden, also ob es sich um Namen, Adressen, Geburtsdaten oder ähnliches handelt, zum anderen erhält er eine Information darüber, an welcher Position der übertragenen Daten Datenbestandteile ausgeschlossen wurden. Diese Information kann insbesondere bei der Wartung von Anwendungsprogrammen wichtig sein, deren Funktionsweise davon abhängen kann, ob bestimmte Datenfelder befüllt sind oder ob bestimmte Informationen zur Verfügung stehen.

Das Datenschutzmodul 13 weist insbesondere für Fernwartungszwecke die Möglichkeit auf, Datenanfragen entgegenzunehmen und zu bearbeiten. Zu diesem Zweck kann es über eine Datenverbindung die Anfrage eines Fernwartungs-Rechners 17 entgegennehmen. Mit der Anfrage werden Identifikationsdaten des Fernwartungsrechners 17 übertragen, die das Datenschutzmodul 13 durch Vergleich mit Identifikationsdaten prüft, die es aus

einem Identifikationsspeicher abruft. Der Identifikationsspeicher ist in das Datenschutzmodul 13 als nicht löschbarer Speicher integriert oder als externer Speicher, z.B. im Anwendungsrechner, zugreifbar. Konnte der Fernwartungsrechner 17 identifiziert werden, leitet das Datenschutzmodul 13 die Datenanfrage an den Anwendungsrechner 3, 5, 7 über eine dafür vorgesehene Datenverbindung weiter. Daraufhin nimmt es die zu übertragenden Daten über eine dafür vorgesehene Datenverbindung entgegen und leitet sie an den Fernwartungsrechner 17 weiter, wobei geheimzuhaltende Datenbestandteile von der Übertragung ausgeschlossen werden.

Figur 2 zeigt ein Verfahren für die Fernübertragung von sensiblen Daten gemäß der Erfindung. In Schritt 31 erfolgt die Anforderung von Daten durch einen entfernt bzw. getrennt angeordneten Rechner 17, 21 oder einen Benutzer einer bestimmten Rolle, d.h. eines bestimmten Autorisierungsstatus, an einen Anwendungsrechner 3, 5, 7 zur Fernübertragung oder Betrachtung von Daten. In Schritt 33 wird geprüft, ob die vollständige Übertragung sämtlicher Daten an den anfragenden Rechner gestattet ist, gegebenenfalls erfolgt diese vollständige Übertragung in Schritt 35, andernfalls wird in Schritt 37 geprüft, ob die zu übertragenden Daten sensible Datenbestandteile enthalten. Die Überprüfung auf sensible Datenbestandteile erfolgt entweder anhand einer entsprechenden Kennung der zu übertragenden Dateien oder Akten oder aber anhand der Verwendung von Suchmasken oder durch Vergleich mit dem Inhalt von Referenzdatenbanken.

In Schritt 39 werden sämtliche geheimhaltungsbedürftige Datenbestandteile der zu übertragenden Daten auf diese Weise erkannt und in Schritt 41 entweder gelöscht, anonymisiert oder pseudonymisiert. Welche der drei Möglichkeiten durchgeführt wird und welche Formate oder Pseudonyme verwendet werden, wird dabei anhand der in einer Datenbank 42 enthaltenen Anonymisierungs-Vorgaben ermittelt. Dabei wird abhängig von der Art der zu übertragenden Daten, z.B. ob es Dateien oder

Kommunikationsdaten wie E-Mail oder Chat sind, und abhängig vom Inhalt der Daten, z.B. ob es Patientenakten oder Bilddaten sind, entschieden, welche der drei Varianten gewählt wird.

Im folgenden Schritt 43 wird geprüft, ob die zu übertragenden Daten Bildschirmdaten oder Videoframes enthalten. Gegebenenfalls wird in Schritt 45 anhand geeigneter Routinen untersucht, ob diese Bildschirminhalte oder Videoframes geheimhaltungsbedürftige Daten in einem ASCII-verwandten Format oder in einem auf ASCII zurückgeführten Format enthalten. Falls ja werden diese geheimhaltungsbedürftigen Daten in Schritt 47 erkannt und im folgenden Schritt 49 von der Übertragung ausgeschlossen. Zu diesem Zweck wird auf eine Anonymisierungsdatenbank 51 zugegriffen, die Vorgaben darüber enthält, ob und in welcher Art die geheimhaltungsbedürftigen Datenbestandteile gelöscht, anonymisiert oder pseudonomysiert werden sollen. In Schritt 53 erfolgt die Übertragung der angeforderten Daten, wobei sämtliche geheimhaltungsbedürftigen Datenbestandteile durch das vorangegangene Verfahren von der Übertragung ausgeschlossen wurden.

Das Verfahren gemäß der Erfindung eignet sich in besonderer Weise für die Fernwartung von Anwendungsrechnern 3, 5, 7 in Arbeitsumgebungen 1 mit sensiblen Daten, da das Verfahren in Schritt 31 durch die Fernabfrage eines Fernwartungsrechners 17 initiiert werden kann. Zu diesem Zweck kann eine Identifikation des Fernwartungsrechners an den Anfang des Verfahrens gestellt werden, durch die sichergestellt werden kann, dass nur authorisierte Fernwartungsrechner 17, 21 Zugriff auf die sensiblen Daten und Anwendungsrechner 3, 5, 7 erhalten.

Patentansprüche

1. Verfahren für die Fernübertragung und/oder Betrachtung sensibler Daten (53) eines Anwendungs-Rechners (3, 5, 7) dadurch gekennzeichnet, dass die Fernübertragung und/oder Betrachtung der sensiblen Daten angefordert wird, dass geheimhaltungsbedürftige Datenbestandteile der angeforderten Daten, z.B. Daten zur Identifizierung von Personen, identifiziert werden, und dass die identifizierten Datenbestandteile von der Fernübertragung (53) und/oder Betrachtung ausgeschlossen werden (41, 49).

2. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass die identifizierten Datenbestandteile durch Löschung, Anonymisierung und/oder Pseudonymisierung (41, 49) ausgeschlossen werden.

3. Verfahren nach einem der vorhergehenden Ansprüche dadurch gekennzeichnet, dass die geheimhaltungsbedürftigen Datenbestandteile durch Vergleich mit dem Inhalt einer Referenzdatenbank, z.B. Namensdatenbank, Adressdatenbank und/oder Personendatenbank, identifiziert werden.

4. Verfahren nach einem der vorhergehenden Ansprüche dadurch gekennzeichnet, dass die geheimhaltungsbedürftigen Datenbestandteile durch Vergleich mit einer Suchmaske, z.B. für ein Datumsangaben-Format und/oder ein Adressangaben-Format, identifiziert werden.

5. Verfahren nach einem der vorhergehenden Ansprüche dadurch gekennzeichnet, dass die geheimhaltungsbedürftigen Datenbestandteile anhand ihrer Position innerhalb der sensiblen Daten, z.B. in einem Namens-Datenfeld und/oder einem Adress-Datenfeld, identifiziert werden.

6. Verfahren nach einem der vorhergehenden Ansprüche d a d u r c h g e k e n n z e i c h n e t , dass die sensiblen Daten einen Bildschirminhalt und/oder ein Video-Frame umfassen.

7. Verfahren nach einem der vorhergehenden Ansprüche d a d u r c h g e k e n n z e i c h n e t , dass die Daten auf Anforderung (31) eines entfernt angeordneten Rechners (17) zur Fernwartung des Anwendungs-Rechners übertragen (53) werden.

8. Datenschutz-Modul (13) für die Fernübertragung und/oder Betrachtung sensibler Daten eines Anwendungs-Rechners (3, 5, 7)
d a d u r c h g e k e n n z e i c h n e t , dass die Fernübertragung und/oder Betrachtung sensibler Daten anforderbar ist, dass die sensiblen Daten in Abhängigkeit von einer solchen Anforderung vom Anwendungs-Rechner (3, 5, 7) an das Datenschutz-Modul (13) übertragbar sind, dass durch das Datenschutz-Modul (13) geheimhaltungsbedürftige Datenbestandteile der Daten, z.B. Name, Alter und/oder Adresse, identifizierbar sind, und dass die identifizierten Datenbestandteile durch das Datenschutz-Modul (13) von der Fernübertragung (53) und/oder Betrachtung ausschließbar (41, 49) sind.

9. Datenschutz-Modul (13) nach Anspruch 8
d a d u r c h g e k e n n z e i c h n e t , dass es als Karte ausgeführt ist, die in den Anwendungs-Rechner (3, 5, 7) einsteckbar ist, oder als Gerät, das an den Anwendungs-Rechner (3, 5, 7) anschließbar ist, oder als integraler Bestandteil des Anwendungs-Rechners (3, 5, 7).

10. Datenschutz-Modul (13) nach Anspruch 8 oder 9
d a d u r c h g e k e n n z e i c h n e t , dass die identifizierten Datenbestandteile durch das Datenschutz-Modul (13) löschbar, anonymisierbar und/oder pseudonymisierbar (41, 49) sind.

11. Datenschutz-Modul (13) nach Anspruch 8, 9 oder 10 d a d u r c h g e k e n n z e i c h n e t , dass es Zugriff auf eine Referenzdatenbank, z.B. Namensdatenbank, Adressdatenbank und/oder Personendatenbank, hat, und dass durch das Datenschutz-Modul (13) die geheimhaltungsbedürftigen Datenbestandteile durch Vergleich mit dem Inhalt der Referenzdatenbank identifizierbar sind.

12. Datenschutz-Modul (13) nach Anspruch 8, 9, 10 oder 11 d a d u r c h g e k e n n z e i c h n e t , dass es Zugriff auf einen Suchmaskenspeicher, z.B. für eine Datums-Suchmaske und/oder eine Adressangaben-Suchmaske, hat, und dass durch das Datenschutz-Modul (13) die geheimhaltungsbedürftigen Datenbestandteile durch Vergleich mit dem Inhalt einer Suchmaske identifizierbar sind.

13. Datenschutz-Modul (13) nach Anspruch 8, 9, 10, 11 oder 12 d a d u r c h g e k e n n z e i c h n e t , dass die geheimhaltungsbedürftigen Datenbestandteile der Daten durch das Datenschutz-Modul (13) anhand ihrer Position innerhalb der sensiblen Daten, z.B. in einem Namens-Datenfeld und/oder einem Adress-Datenfeld, identifizierbar sind.

14. Datenschutz-Modul (13) nach Anspruch 8, 9, 10, 11, 12 oder 13
d a d u r c h g e k e n n z e i c h n e t , dass die geheimhaltungsbedürftigen Datenbestandteile durch das Datenschutz-Modul (13) in sensiblen Daten, die einen Bildschirminhalt und/oder ein Video-Frame repräsentieren, identifizierbar sind.

15. Datenschutz-Modul (13) nach Anspruch 8, 9, 10, 11, 12, 13 oder 14
d a d u r c h g e k e n n z e i c h n e t , dass es einen Daten-Anschluss aufweist, über den eine Anforderung eines entfernt angeordneten Rechners (17, 21) zur Übertragung der

sensiblen Daten empfangbar ist, dass es einen Daten-Anschluss aufweist, über den diese Anforderung an einen Anwendungs-Rechner (3, 5, 7) übertragbar ist, dass es einen Daten-Anschluss aufweist, über den die sensiblen Daten vom Anwendungs-Rechner (3, 5, 7) empfangbar sind, und dass es einen Daten-Anschluss aufweist, über den Daten an den entfernt angeordneten Rechner (17, 21) übertragbar sind.

16. Datenschutz-Modul (13) nach Anspruch 15 d a d u r c h g e k e n n z e i c h n e t , dass es Zugriff auf einen Speicher hat, der Identifikations-Daten zur Identifikation eines entfernt angeordneten Wartungs-Rechners (17, 21) enthält, dass durch das Datenschutz-Modul (13) ein Rechner (17, 21) unter Verwendung der Identifikations-Daten identifizierbar ist, und dass Daten nur in Abhängigkeit vom Ergebnis der Identifikation an einen entfernt angeordneten Rechner (17, 21) übertragbar sind.

Zusammenfassung

Verfahren und Vorrichtung für die Fernübertragung sensibler Daten

Die Erfindung betrifft ein Verfahren für die Fernübertragung und/oder Betrachtung sensibler Daten (53) eines Anwendungs-Rechners (3, 5, 7). Gemäß der Erfindung erfolgt die Fernübertragung und/oder Betrachtung der sensiblen Daten auf Anforderung. Vor der Fernübertragung (53) und/oder Betrachtung werden geheimhaltungsbedürftige Datenbestandteile der angeforderten Daten,. z.B. Daten zur Identifizierung von Personen, identifiziert und eliminiert (41, 49). Die Erfindung betriff außerdem ein Datenschutz-Modul (13) für die Fernübertragung und/oder Betrachtung sensibler Daten eines Anwendungs-Rechners (3, 5, 7). Gemäß der Erfindung ist die Fernübertragung und/oder Betrachtung sensibler Daten anforderbar. Auf eine solche Anforderung hin sind die sensiblen Daten vom Anwendungs-Rechner (3, 5, 7) an das Datenschutz-Modul (13) übertragbar. Geheimhaltungsbedürftige Datenbestandteile der Daten, z.B. Name, Alter und/oder Adresse, sind durch das Datenschutz-Modul (13) identifizierbar und von der Fernübertragung (53) und/oder Betrachtung ausschließbar (41, 49).

FIG 1

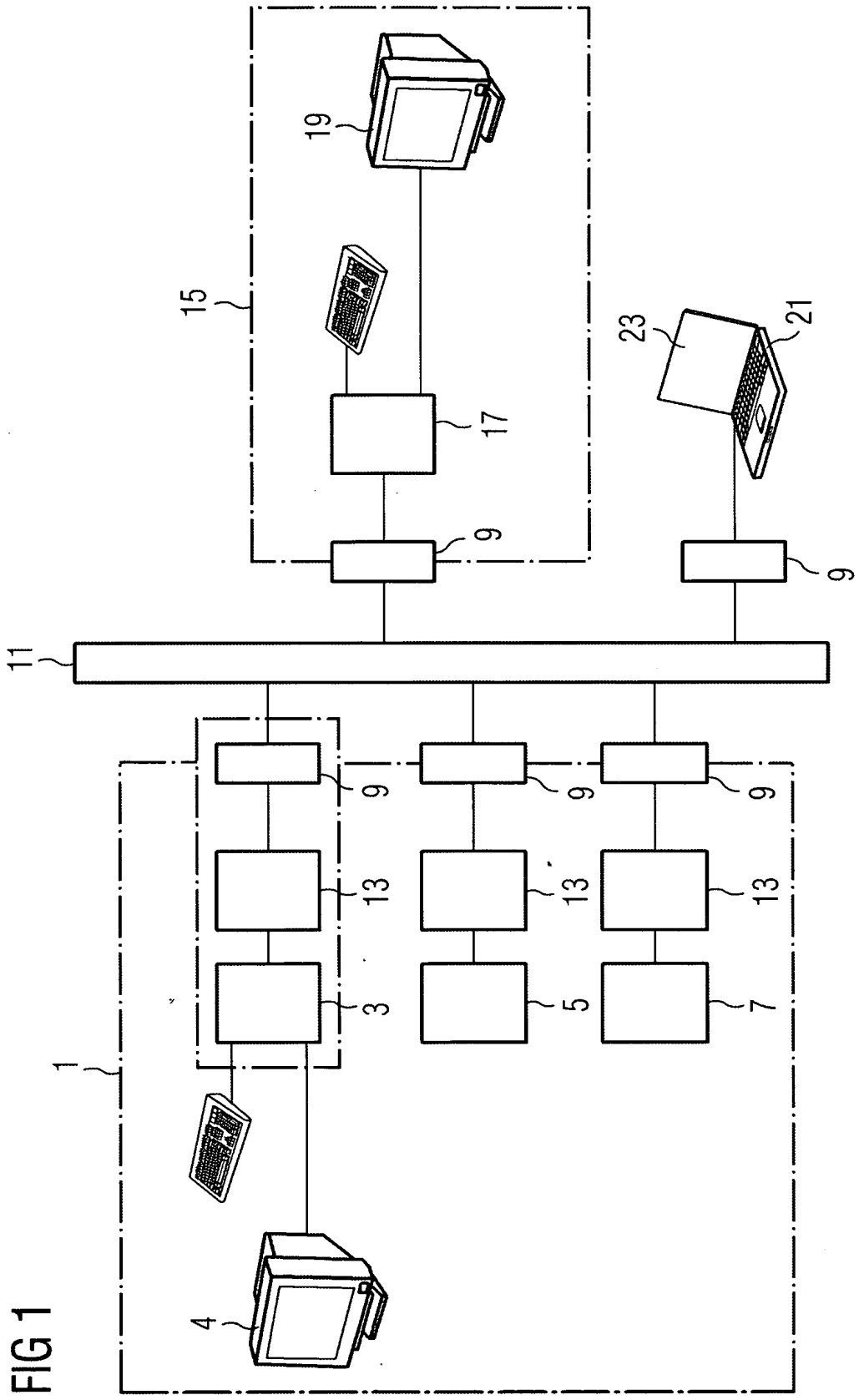

FIG 1

FIG 2